(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
26 février 2004 (26.02.2004)

PCT

(10) Numéro de publication internationale
WO 2004/017193 A3

(51) Classification internationale des brevets[7] : G06F 7/72

(21) Numéro de la demande internationale :
PCT/FR2003/002462

(22) Date de dépôt international : 5 août 2003 (05.08.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/10193 9 août 2002 (09.08.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : GEMPLUS [FR/FR]; Département Brevets, La Vigie, Boîte postale 90, F-13705 La Ciotat Cedex (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : BILLET, Olivier [FR/FR]; 1211, route des Vallettes Sud, F-06140 Tourrettes sur Loup (FR). JOYE, Marc [FR/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR).

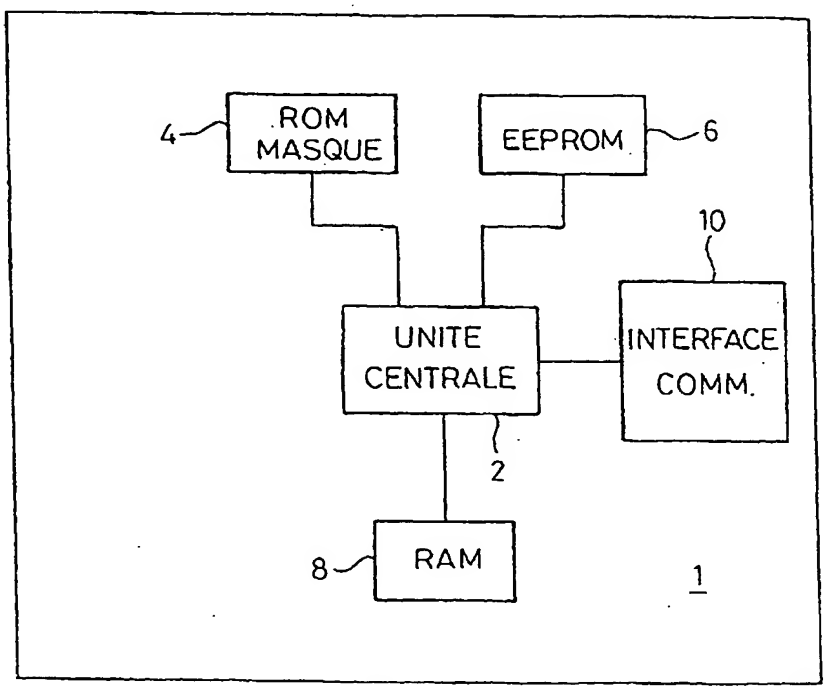
(74) Mandataire : BRUYERE, Pierre; Gemplus, Service Brevèts, La Vigie, Boîte postale 90, F-13705 La Ciotat Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD,

[Suite sur la page suivante]

(54) Title: METHOD FOR UNIVERSAL CALCULATION APPLIED TO POINTS OF AN ELLIPTIC CURVE

(54) Titre : PROCEDE DE CALCUL UNIVERSEL APPLIQUE A DES POINTS D'UNE COURBE ELLIPTIQUE



2... CENTRAL UNIT
4...MASK ROM
6...EEPROM
8...RAM
10...COMMUNICATION INTERFACE

(57) Abstract: The invention concerns a method for universal calculation on the points of an elliptic curve. The invention is characterized in that the elliptic curve is defined by a quartic equation and identical programmed calculating means are used for operating an addition of points, a doubling of points and an addition of a neutral point, the calculating means comprising in particular a central unit (2) associated with a memory (4, 6, 8). The invention also concerns a cryptographic method using such a universal method. The invention further concerns a component for implementing the universal calculation method and/or the cryptographic method. For example, the invention is applicable to smart cards.

(57) Abrégé : L'invention concerne un procédé de calcul universel sur des points d'une courbe elliptique. Selon l'invention, la courbe elliptique est définie par une équation quartique et des moyens de calcul programmés identiques sont utilisés pour réaliser une opération d'addition de points,

[Suite sur la page suivante]

WO 2004/017193 A3